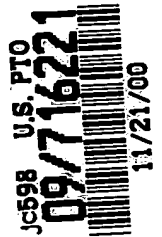


#3
THE COMMISSIONER IS AUTHORIZED
TO CHARGE ANY DEFICIENCY IN THE
FEES FOR THIS PAPER TO DEPOSIT
ACCOUNT NO. 23-0975

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of :
Hisashi INOUE et al. :
Serial No. NEW : Attn: APPLICATION BRANCH
Filed November 21, 2000 : Attorney Docket No. 2000_1451A



APPARATUS AND METHOD FOR EMBEDDING
INFORMATION FOR TAMPER DETECTION
AND DETECTING TAMPER AND RECORDING
MEDIUM HAVING PROGRAM FOR CARRYING
OUT THE METHOD RECORDED THEREON

CLAIM OF PRIORITY UNDER 35 USC 119

Assistant Commissioner for Patents,
Washington, DC 20231

Sir:

Applicants in the above-entitled application hereby claim the date of priority under the International Convention of Japanese Patent Application No. 11-333775, filed November 25, 1999, as acknowledged in the Declaration of this application.

A certified copy of said Japanese Patent Application is submitted herewith.

Respectfully submitted,

Hisashi INOUE et al.

By Charles R. Watts
Charles R. Watts
Registration No. 33,142
Attorney for Applicants

CRW/asd
Washington, D.C. 20006
Telephone (202) 721-8200
Facsimile (202) 721-8250
November 21, 2000

日 本 国 特 許 庁

PATENT OFFICE
JAPANESE GOVERNMENT



別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application:

1 9 9 9 年 1 1 月 2 5 日

出 願 番 号
Application Number:

平成 1 1 年 特 許 願 第 3 3 3 7 7 5 号

出 願 人
Applicant (s):

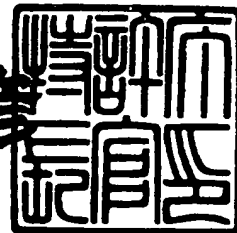
松下電器産業株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

2 0 0 0 年 6 月 2 3 日

特 許 庁 長 官
Commissioner,
Patent Office

近 藤 隆 彦



【書類名】 特許願
【整理番号】 2038610041
【提出日】 平成11年11月25日
【あて先】 特許庁長官殿
【国際特許分類】 H04N 1/387
G09C 5/00
G06T 9/00

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 井上 尚

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 桂 卓史

【特許出願人】

【識別番号】 000005821

【氏名又は名称】 松下電器産業株式会社

【代理人】

【識別番号】 100097445

【弁理士】

【氏名又は名称】 岩橋 文雄

【選任した代理人】

【識別番号】 100103355

【弁理士】

【氏名又は名称】 坂口 智康

【選任した代理人】

【識別番号】 100109667

【弁理士】

【氏名又は名称】 内藤 浩樹

【手数料の表示】

【予納台帳番号】 011305

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9809938

【プルーフの要否】 不要

【書類名】 明細書

【発明の名称】 デジタル画像の改ざん防止装置および方法並びに当該方法を実施するプログラムを記録した記録媒体

【特許請求の範囲】

【請求項 1】 デジタル画像信号を複数の周波数帯域に分割する帯域分割手段と、予め定めた鍵データを用いて疑似乱数系列を作成し、当該疑似乱数系列から認証データを作成する認証データ作成手段と、前記複数の周波数帯域のうち、最も低い周波数帯域（以下、M R A という）の変換係数に前記鍵データを埋め込む鍵情報埋込み手段と、M R A 以外の周波数帯域（以下、M R R という）の変換係数に前記認証データを埋め込む認証データ埋込み手段と、情報埋め込み後の前記 M R A と前記 M R R を用いて、情報の埋め込みがなされたデジタル画像信号を再構成する帯域合成手段とを備えたことを特徴とする改ざん防止装置。

【請求項 2】 デジタル画像信号を複数の周波数帯域に分割する帯域分割手段と、前記複数の周波数帯域のうち、M R A の変換係数から鍵データを抽出する鍵情報抽出手段と、前記鍵データを用いて疑似乱数系列を作成し、当該疑似乱数系列から認証データを作成する認証データ作成手段と、前記複数の周波数帯域のうち、M R R の変換係数から埋込み情報を抽出する埋込み情報抽出手段と、前記認証データと抽出した前記埋込み情報とを比較照合して改ざんの有無を判定する改ざん判定手段とを備えたことを特徴とする改ざん防止装置。

【請求項 3】 正の数である第 1 の設定値および第 1 の設定値より小さい正の数を第 2 の設定値 m として予め定め、前記認証データ埋込み手段は、変換係数の絶対値と第 1 の設定値とを比較し、前記変換係数の絶対値が第 1 の設定値より小さい場合、変換係数に対応する認証データのビット値に応じて、前記変換係数を m または $-m$ に設定する第 1 の埋込み手段と、前記変換係数を量子化ステップサイズ Q で割った値を q として予め定め、前記変換係数の絶対値が第 1 の設定値以上の場合、変換係数に対応する認証データのビット値に応じて、前記 q の値を最も近い偶数または奇数の整数値に設定する第 2 の埋込み手段とを備え、前記認証データを M R R の変換係数に埋め込むことを特徴とする請求項 1 に記載の改ざん防止装置。

【請求項 4】 前記埋込み情報抽出手段は、変換係数の絶対値と前記第 1 の設定値とを比較し、前記変換係数の絶対値が前記第 1 の設定値より小さい場合、前記変換係数の値が正か負かを判定し、当該判定の結果に基づいて変換係数毎に埋込まれた情報のビット値を抽出する第 1 の抽出手段と、前記変換係数を量子化ステップサイズ Q で割り四捨五入した値を p として予め定め、前記変換係数の絶対値が前記第 1 の設定値以上の場合、前記 p の値が偶数か奇数かを判定し、当該判定の結果に基づいて変換係数毎に埋込まれた情報のビット値を抽出する第 2 の抽出手段とを備え、前記 M R R の変換係数から埋込み情報を抽出することを特徴とする請求項 2 または 3 に記載の改ざん防止装置。

【請求項 5】 前記改ざんの有無を判定する改ざん判定手段は、デジタル画像を予め定めた複数の画素から構成される複数のブロックに分割するブロック分割手段と、ブロックと同一の空間的領域を表現する M R R 内に埋め込まれている埋込み情報の系列を前記抽出した埋込み情報の中から読み出す領域対応埋込情報読出手段と、前記認証データの中から、前記読み出した埋込み情報と同じ位置に対応する認証データの系列を読み出す領域対応認証データ読出手段と、前記ブロック毎に読み出された前記埋込み情報の系列と前記認証データの系列とを比較することによって、当該ブロックの改ざんの有無を判定するブロック改ざん判定手段とを備えたことを特徴とする請求項 2 に記載の改ざん防止装置。

【請求項 6】 デジタル画像信号を複数の周波数帯域に帯域分割するステップと、予め定めた鍵データを用いて疑似乱数系列を作成し、当該疑似乱数系列から認証データを作成するステップと、前記複数の周波数帯域のうち、最も低い周波数帯域（以下、M R A という）の変換係数に前記鍵データを埋め込むステップと、M R A 以外の周波数帯域（以下、M R R という）の変換係数に前記認証データを埋め込むステップと、情報埋め込み後の前記 M R A と前記 M R R を用いて、情報の埋め込みがなされたデジタル画像信号を再構成するステップとを備えたことを特徴とする改ざん防止方法。

【請求項 7】 デジタル画像信号を複数の周波数帯域に帯域分割するステップと、前記複数の周波数帯域のうち、M R A の変換係数から鍵データを抽出するステップと、前記鍵データを用いて疑似乱数系列を作成し、当該疑似乱数系列から

認証データを作成するステップと、前記複数の周波数帯域のうち、M R Rの変換係数から埋込み情報を抽出するステップと、前記認証データと抽出した前記埋込み情報を比較照合して改ざんの有無を判定するステップとを備えたことを特徴とする改ざん防止方法。

【請求項 8】 正の数である第 1 の設定値および第 1 の設定値より小さい正の数を第 2 の設定値 m として予め定め、前記 M R R の変換係数に埋め込むステップは、変換係数の絶対値と第 1 の設定値とを比較し、前記変換係数の絶対値が第 1 の設定値より小さい場合、変換係数に対応する認証データのビット値に応じて、前記変換係数を m または $-m$ に設定するステップと、前記変換係数を量子化ステップサイズ Q で割った値を q として予め定め、前記変換係数の絶対値が第 1 の設定値以上の場合、変換係数に対応する認証データのビット値に応じて、前記 q の値を最も近い偶数または奇数の整数値に設定するステップとを備え、前記認証データを M R R の変換係数に埋め込むことを特徴とする請求項 6 に記載の改ざん防止方法。

【請求項 9】 前記 M R R の変換係数から埋込み情報を抽出するステップは、変換係数の絶対値と前記第 1 の設定値とを比較し、前記変換係数の絶対値が前記第 1 の設定値より小さい場合、前記変換係数の値が正か負かを判定し、当該判定の結果に基づいて変換係数毎に埋込まれた情報のビット値を抽出するステップと、前記変換係数を量子化ステップサイズ Q で割り四捨五入した値を p として予め定め、前記変換係数の絶対値が前記第 1 の設定値以上の場合、前記 p の値が偶数か奇数かを判定し、当該判定の結果に基づいて変換係数毎に埋込まれた情報のビット値を抽出するステップとを備え、前記 M R R の変換係数から埋込み情報を抽出することを特徴とする請求項 7 または 8 に記載の改ざん防止方法。

【請求項 1 0】 前記改ざんの有無を判定するステップは、デジタル画像を予め定めた複数の画素から構成される複数のブロックに分割するステップと、ブロックと同一の空間的領域を表現する M R R 内に埋め込まれている埋込み情報の系列を前記抽出した埋込み情報の中から読み出すステップと、前記認証データの中から、前記読み出した埋込み情報と同じ位置に対応する認証データの系列を読み出すステップと、前記ブロック毎に読み出された前記埋込み情報の系列と前記認

証データの系列とを比較することによって、当該ブロックの改ざんの有無を判定するステップとを備えたことを特徴とする請求項 7 に記載の改ざん防止方法。

【請求項 1 1】 デジタル画像信号を複数の周波数帯域に帯域分割するステップと、予め定めた鍵データを用いて疑似乱数系列を作成し、当該疑似乱数系列から認証データを作成するステップと、前記複数の周波数帯域のうち、最も低い周波数帯域（以下、M R A という）の変換係数に前記鍵データを埋め込むステップと、M R A 以外の周波数帯域（以下、M R R という）の変換係数に前記認証データを埋め込むステップと、情報埋め込み後の前記 M R A と前記 M R R を用いて、情報埋め込みがなされたデジタル画像信号を再構成するステップを実行するためのプログラムを記録した記録媒体。

【請求項 1 2】 デジタル画像信号を複数の周波数帯域に帯域分割するステップと、前記複数の周波数帯域のうち、M R A の変換係数から鍵データを抽出するステップと、前記鍵データを用いて疑似乱数系列を作成し、当該疑似乱数系列から認証データを作成するステップと、前記複数の周波数帯域のうち、M R R の変換係数から埋込み情報を抽出するステップと、前記認証データと抽出した前記埋込み情報を比較照合して改ざんの有無を判定するステップを実行するためのプログラムを記録した記録媒体。

【請求項 1 3】 正の数である第 1 の設定値および第 1 の設定値より小さい正の数を第 2 の設定値 m として予め定め、前記 M R R の変換係数に埋め込むステップは、変換係数の絶対値と第 1 の設定値とを比較し、前記変換係数の絶対値が第 1 の設定値より小さい場合、変換係数に対応する認証データのビット値に応じて、前記変換係数を m または $-m$ に設定するステップと、前記変換係数を量子化ステップサイズ Q で割った値を q として予め定め、前記変換係数の絶対値が第 1 の設定値以上の場合、変換係数に対応する認証データのビット値に応じて、前記 q の値を最も近い偶数または奇数の整数値に設定するステップとを備え、前記認証データを M R R の変換係数に埋め込むことを特徴とする請求項 1 1 に記載の記録媒体。

【請求項 1 4】 前記 M R R の変換係数から埋込み情報を抽出するステップは、変換係数の絶対値と前記第 1 の設定値とを比較し、前記変換係数の絶対値が前

記第 1 の設定値より小さい場合、前記変換係数の値が正か負かを判定し、当該判定の結果に基づいて変換係数毎に埋込まれた情報のビット値を抽出するステップと、前記変換係数を量子化ステップサイズ Q で割り四捨五入した値を p として予め定め、前記変換係数の絶対値が前記第 1 の設定値以上の場合、前記 p の値が偶数か奇数かを判定し、当該判定の結果に基づいて変換係数毎に埋込まれた情報のビット値を抽出するステップとを備え、前記 M R R の変換係数から埋込み情報を抽出することを特徴とする請求項 1 2 または 1 3 に記載の記録媒体。

【請求項 1 5】 前記改ざんの有無を判定するステップは、デジタル画像を予め定めた複数の画素から構成される複数のブロックに分割するステップと、ブロックと同一の空間的領域を表現する M R R 内に埋め込まれている埋込み情報の系列を前記抽出した埋込み情報の中から読み出すステップと、前記認証データの中から、前記読み出した埋込み情報と同じ位置に対応する認証データの系列を読み出すステップと、前記ブロック毎に読み出された前記埋込み情報の系列と前記認証データの系列とを比較することによって、当該ブロックの改ざんの有無を判定するステップとを備えたことを特徴とする請求項 1 2 に記載の記録媒体。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、デジタル画像の改ざん防止装置および方法並びに記憶媒体に関し、より特定的には、デジタル画像の部分的な改ざんの有無及び改ざん位置を検出するために、デジタル画像信号に認証データを埋め込み、そして抽出する改ざん防止装置および方法並びに記憶媒体に関する。

【0 0 0 2】

【従来の技術】

近年、インターネットを利用した情報の提供が盛んになっている。特に WWW (World Wide Web) は、画像や音声などを統合した情報送受信サービスとして頻繁に利用されている。しかしながら、こうしたオープンなネットワーク環境では、不特定多数の者が画像などのデジタル情報を容易にコピーすることができる。しかも、市販の画像処理ソフトウェアを利用して簡単にデジタル

画像を編集・加工することができ、デジタル画像が第三者によって改ざんされ、受信者は改ざんされたことに気付かれない場合が想定される。そこで、配信されたデジタル画像に改ざんが加えられているか否か判定できる改ざん検出技術の確立が求められている。従来、その対策の一つとして知られているものに電子認証技術がある。

【 0 0 0 3 】

図 1 4 は、従来の電子認証の手順の概要を示した説明図である。送信側では、オリジナルのデジタル画像に対してハッシュ関数を適用してデータ圧縮したダイジェストを送り手による秘密鍵で暗号化する。そして、オリジナルのデジタル画像及び暗号化されたダイジェストをネットワークを通して受信側に送信する。受信側では、ネットワークより受信したデジタル画像に対してハッシュ関数によるデータ圧縮を行ってダイジェストを作成すると共に、暗号化されたダイジェストに対して送り手の公開鍵による復号化を行ってダイジェストを復号する。そして、オリジナルのデジタル画像から作成したダイジェストと復号したダイジェストとを比較し、両方のダイジェストが同一であれば改ざんが行われていないと判定し、逆に、異なっていれば改ざんが行われていると判定する。

【 0 0 0 4 】

ところが、上述のようにして電子認証を行う場合、送信側では、オリジナルのデジタル画像及び暗号化されたダイジェストの 2 種類のデータを受信側へ送信する必要があるが、デジタル画像が大量の場合には、ネットワークを通して送信する際に、どのデジタル画像に対してどのダイジェストが対応しているのかを送信側で適切に管理するためのデータ管理手段が別途必要になる。このようなデータ管理手段の代わりとして、従来、電子透かし技術を用いた手法がある。

【 0 0 0 5 】

電子透かしとは、デジタル画像データ内部に人間には知覚できないような形でデジタル情報を埋め込む技術である。電子透かし技術により、例えば、デジタル画像の上位ビットからダイジェストを作成し、これを送り手による秘密鍵で暗号化する。そして、デジタル画像の各画素の下位ビットに暗号化したダイジェストを埋め込む。受信側では送信されたデジタル画像の下位ビットに埋め込まれてい

る暗号化ダイジェストを抽出し、送り手の公開鍵による復号化を行ってダイジェストを復号する。一方、受信したデジタル画像の上位ビットから直接照合用ダイジェストを作成する。そして、照合用ダイジェストと復号したダイジェストとを比較し、両方のダイジェストが同一であれば改ざんが行われていないと判定し、逆に、異なっていれば改ざんが行われていると判定する。

【0006】

【発明が解決しようとする課題】

しかしながら、従来の電子透かし技術では、送信途中でデジタル画像が改ざんされたことを受信側で発見できても、デジタル画像中のどの部分が改ざんされたかを特定することができないという課題があった。また、電子透かし方式では、一般に人間の目には知覚しにくい高周波成分を利用してダイジェストの埋め込みを行っているので、J P E Gなどの非可逆な画像圧縮伸長を行った場合、埋め込んだ情報に変化してしまい、正しく読み出せない。すなわち、悪意を持った者によるデジタル画像の一部を改変した場合と一般的に行う非可逆的な画像圧縮とによるデジタル画像の改ざんの区別ができないという課題があった。さらに、画像の高周波成分に対応する部分は、一般的にエッジやテクスチャ部分であるため、平坦な部分が多い画像では、画像全体に情報が埋め込まれないことになる。その結果、平坦部分を改ざんした場合は、検出できないことが発生する可能性がある。

【0007】

それ故、本発明の目的は、画像の高周波成分だけではなく、画像全体に情報を埋め込む。すなわち、比較的低周波成分の変換係数に情報を埋め込むことにより、非可逆的な圧縮と画像の一部を改ざんする行為とを区別することができ、しかも改ざん部分の特定が可能なデジタル画像の改ざん防止装置及び方法を提供することである。

【0008】

【課題を解決するための手段】

第1の発明は、デジタル画像信号を複数の周波数帯域に分割する帯域分割手段と、予め定めた鍵データを用いて疑似乱数系列を作成し、当該疑似乱数系列から

認証データを作成する認証データ作成手段と、複数の周波数帯域のうち、最も低い周波数帯域（以下、M R A という）の変換係数に前記鍵データを埋め込む鍵情報埋込み手段と、M R A 以外の周波数帯域（以下、M R R という）の変換係数に前記認証データを埋め込む認証データ埋込み手段と、情報埋め込み後の前記M R A と前記M R R を用いて、情報の埋め込みがなされたデジタル画像信号を再構成する帯域合成手段とを備える。

【 0 0 0 9 】

第 2 の発明は、デジタル画像信号を複数の周波数帯域に分割する帯域分割手段と、前記複数の周波数帯域のうち、M R A の変換係数から鍵データを抽出する鍵情報抽出手段と、前記鍵データを用いて疑似乱数系列を作成し、当該疑似乱数系列から認証データを作成する認証データ作成手段と、前記複数の周波数帯域のうち、M R R の変換係数から埋込み情報を抽出する埋込み情報抽出手段と、前記認証データと抽出した前記埋込み情報とを比較照合して改ざんの有無を判定する改ざん判定手段とを備える。

【 0 0 1 0 】

第 3 の発明は、第 1 の発明に従属する発明であって、正の数である第 1 の設定値および第 1 の設定値より小さい正の数を第 2 の設定値 m として予め定め、変換係数の絶対値と第 1 の設定値とを比較し、前記変換係数の絶対値が第 1 の設定値より小さい場合、変換係数に対応する認証データのビット値に応じて、前記変換係数を m または $-m$ に設定する第 1 の埋込み手段と、前記変換係数を量子化ステップサイズ Q で割った値を q として予め定め、前記変換係数の絶対値が第 1 の設定値以上の場合、変換係数に対応する認証データのビット値に応じて、前記 q の値を最も近い偶数または奇数の整数値に設定する第 2 の埋込み手段とを備え、前記認証データを M R R の変換係数に埋め込むことを特徴とする。

【 0 0 1 1 】

第 4 の発明は、第 2 または第 3 の発明に従属する発明であって、変換係数の絶対値と前記第 1 の設定値とを比較し、前記変換係数の絶対値が前記第 1 の設定値より小さい場合、前記変換係数の値が正か負かを判定し、当該判定の結果に基づいて変換係数毎に埋込まれた情報のビット値を抽出する第 1 の抽出手段と、前記

変換係数を量子化ステップサイズQで割り四捨五入した値をpとして予め定め、前記変換係数の絶対値が前記第1の設定値以上の場合、前記pの値が偶数か奇数かを判定し、当該判定の結果に基づいて変換係数毎に埋込まれた情報のビット値を抽出する第2の抽出手段とを備え、前記MRRの変換係数から埋込み情報を抽出することを特徴とする。

【0012】

第5の発明は、第2の発明に従属する発明であって、デジタル画像を予め定めた複数の画素から構成される複数のブロックに分割するブロック分割手段と、ブロックと同一の空間的領域を表現するMRR内に埋め込まれている埋込み情報の系列を抽出した埋込み情報の中から読み出す領域対応埋込情報読出手段と、前記認証データの中から、前記読み出した埋込み情報と同じ位置に対応する認証データを読み出す領域対応認証データ読出手段と、前記ブロック毎に読み出された前記埋込み情報の系列と前記認証データの系列とを比較することによって、当該ブロックの改ざんの有無を判定するブロック改ざん判定手段とを備えたことを特徴とする。

【0013】

【発明の実施の形態】

図1および図2は、本発明の実施形態に係るデジタル画像の改ざん防止装置の構成図である。図1は情報埋込み装置1aを示すブロック図、図2は情報抽出装置2aを示すブロック図である。

【0014】

図1において、情報埋込み装置1aは、帯域分割部11と、認証データ作成部12と、鍵情報埋込み部13と、認証データ埋込み部14と、帯域合成部15とを備える。

【0015】

図2において、情報抽出装置2aは、帯域分割部11と、鍵情報抽出部21と、鍵情報判定部22と、認証データ作成部12と、埋込み情報抽出部23と、領域対応埋込情報読出部24と、領域対応認証データ読出部25と、ブロック改ざん判定部26とを備える。

【0016】

なお、本実施形態に係る情報抽出装置 2 a の帯域分割部 1 1 と認証データ作成部 1 2 は、本実施形態に係る情報埋込装置 1 a の帯域分割部 1 1 と認証データ作成部 1 2 と同様の構成であり、以下当該構成について、同一の参照番号を付してその説明を省略する。

【0017】

以下、図 3 ～図 1 3 を参照して、本実施形態に係るデジタル画像の改ざん防止装置が行う改ざん防止方法を順に説明する。

【0018】

まず、情報埋込装置 1 a が行う情報埋込み方法について説明する。図 3 は、図 1 の情報埋込み装置 1 a で行う処理を示すフローチャートである。図 3 を参照して、まず、帯域分割部 1 1 の処理について、図 4 ～図 6 を用いて説明する。

【0019】

図 4 は、従来の離散ウェーブレット変換処理を用いて 3 階層への帯域分割を行う帯域分割部 1 1 の構成の一例を示すブロック図である。図 4 において、帯域分割部 1 1 は、それぞれ同じ構成を有する第 1 ～第 3 の帯域分割フィルタ 1 0 0、2 0 0 および 3 0 0 を備える。第 1 ～第 3 の帯域分割フィルタ 1 0 0、2 0 0 および 3 0 0 は、入力した画像を 4 つの周波数帯域に分割し、各周波数帯域ごとのウェーブレット係数（以下、変換係数という）を算出する（ステップ S 3 0 1）。なお、サブバンド分割によっても、離散ウェーブレット変換による帯域分割と等価である変換係数を得ることもできる。帯域分割部 1 1 は、デジタル画像信号 7 1 を第 1 の帯域分割フィルタ 1 0 0 に入力する。

【0020】

第 1 の帯域分割フィルタ 1 0 0 は、デジタル画像信号 7 1 を水平周波数成分と垂直周波数成分のパラメータに基づいて 4 つの帯域の信号、すなわち、LL 1 信号、LH 1 信号、HL 1 信号および HH 1 信号（以下、これらを総称して第 1 の階層信号という）に分割する。

【0021】

第 2 の帯域分割フィルタ 2 0 0 は、上記第 1 の階層信号のうち最も低域の LL

1 信号を入力し、さらに4つの帯域のLL 2 信号、LH 2 信号、HL 2 信号およびHH 2 信号（以下、これらを総称して第2の階層信号という）に分割する。

【0 0 2 2】

そして、第3の帯域分割フィルタ3 0 0は、上記第2の階層信号のうち最も低域のLL 2 信号を入力し、さらに4つの帯域のLL 3 信号、LH 3 信号、HL 3 信号およびHH 3 信号（以下、これらを総称して第3の階層信号という）に分割する。

【0 0 2 3】

図5は、図4の第1の帯域分割フィルタ1 0 0の構成の一例を示すブロック図である。図5において、第1の帯域分割フィルタ1 0 0は、第1～第3の2帯域分割部1 0 1～1 0 3を備える。この第1～第3の2帯域分割部1 0 1～1 0 3は、それぞれ1次元の低域通過フィルタ（LPF）1 1 1～1 1 3と、1次元の高域通過フィルタ（HPF）1 2 1～1 2 3と、信号を2：1に間引くダウンサンプラ1 3 1～1 3 3および1 4 1～1 4 3とを備える。

【0 0 2 4】

第1の2帯域分割部1 0 1は、デジタル画像信号7 1を入力し、水平方向成分に関してLPF 1 1 1およびHPF 1 2 1により低域および高域のフィルタリングを行い、2つの信号を出力する。そして低域および高域のフィルタリングがされた信号をそれぞれダウンサンプラ1 3 1および1 4 1を用いて2：1に間引いた後、次段に出力する。

【0 0 2 5】

第2の2帯域分割部1 0 2は、ダウンサンプラ1 3 1からの信号を入力し、垂直方向成分に関してLPF 1 1 2およびHPF 1 2 2によりそれぞれフィルタリングを行い、ダウンサンプラ1 3 2および1 4 2を用いて2：1に間引いた後、LL 1 信号とLH 1 信号の2つの信号を出力する。

【0 0 2 6】

一方、第3の2帯域分割部1 0 3は、ダウンサンプラ1 4 1からの信号を入力し、垂直方向成分に関してLPF 1 1 3およびHPF 1 2 3によりそれぞれフィルタリングを行い、ダウンサンプラ1 3 3および1 4 3を用いて2：1に間引い

た後、HL 1 信号とHH 1 信号の 2 つの信号を出力する。

【0 0 2 7】

これにより、第 1 の帯域分割フィルタ 1 0 0 からは、水平方向・垂直方向共に低域の LL 1 信号、水平方向に低域で垂直方向に高域の LH 1 信号、水平方向に高域で垂直方向に低域の HL 1 信号および水平方向・垂直方向共に高域の HH 1 信号の 4 つの信号、すなわち、変換係数が出力される。なお、第 2 および第 3 の帯域分割フィルタ 2 0 0 および 3 0 0 も、入力する信号に対して上記と同様の処理を行う。

【0 0 2 8】

上述した第 1 ～第 3 の帯域分割フィルタ 1 0 0、2 0 0 および 3 0 0 による帯域分割処理の結果、画像信号 7 1 は、LL 3 信号、LH 3 信号、HL 3 信号、HH 3 信号、LH 2 信号、HL 2 信号、HH 2 信号、LH 1 信号、HL 1 信号および HH 1 信号の 1 0 個の周波数帯域に分割される。図 6 は、これらを 2 次元周波数領域で表現した図である。ここで、最も低い周波数帯域 LL 3 信号を MRA、MRA 以外の周波数帯域を MRR という。

【0 0 2 9】

つまり、MRR は、LH 3 信号、HL 3 信号、HH 3 信号、LH 2 信号、HL 2 信号、HH 2 信号、LH 1 信号、HL 1 信号および HH 1 信号を表している。図 6 において、縦軸は垂直方向の周波数成分を表し下側に行くほど高域となり、横軸は水平方向の周波数成分を表し右側に行くほど高域となる。

【0 0 3 0】

図 6 における各々の領域は 1 つの画像としてのデータであり、その領域の面積比は各々の帯域信号が有するデータ数の比に一致する。すなわち、第 3 の階層信号である LL 3 信号、LH 3 信号、HL 3 信号および HH 3 信号のデータ数を 1 とした場合、第 2 の階層信号である LH 2 信号、HL 2 信号および HH 2 信号のデータ数は 4 (2 × 2 サイズ) となり、第 1 の階層信号である LH 1 信号、HL 1 信号および HH 1 信号のデータ数は 1 6 (4 × 4 サイズ) となる。

【0 0 3 1】

従って、例えば、LL 3 信号の左上の 1 個のデータに関しては、LH 3 信号、

HL 3 信号およびHH 3 信号のそれぞれ左上の 1 個のデータが、LH 2 信号、HL 2 信号およびHH 2 信号のそれぞれ左上の正方形の 4 個のデータが、LH 1 信号、HL 1 信号およびHH 1 信号のそれぞれ左上の正方形の 16 個のデータが原画像上での同一画素を表現することとなる（図 6 中、黒で塗りつぶしてある部分である）。つまり、画像信号において左上の正方形の 64 個（ 8×8 サイズ）の画素データは、上記の各周波数帯域の変換係数と同一の空間的領域を表現する。

【0032】

次に、認証データ作成部 12 は、予め定めた鍵データを用いて疑似乱数系列を作成し、当該疑似乱数系列から認証データを作成する（ステップ S302）。具体的には、疑似乱数系列から生成されるランダムな実数値が正か負かを判断し、正の場合はビット値 1 と、負の場合はビット値 0 として認証データを作成する。鍵データとしては、例えば、疑似乱数系列を生成するための初期値、乱数発生関数の種類、系列のビット長を示す情報を含む。本実施の形態では、簡単のために各鍵データはそれぞれ 8 ビットのデータ長で表される値とする。また、以下の説明において、認証データは、ビット値 1 と 0 に 2 進数化されたビットストリームであるとする。鍵データの情報は、埋め込み処理を行うためのキー情報であり、情報を抽出する際にも用いるので、情報埋め込み装置と情報抽出装置の双方側で予め値を決定しておく必要がある。

【0033】

次に、鍵情報埋め込み部 13 は、帯域分割部 11 で分割した信号の MRA の変換係数を予め定めた順序で読み出し、前記鍵データを埋め込む（ステップ S303）。この埋め込み手法として、特開平 1 1 - 1 9 6 2 6 2 号公報に開示された技術を用いる。すなわち、変換係数を量子化ステップサイズ Q で割った値を q とすると、変換係数に対応する鍵データのビット値に応じて、前記 q の値を最も近い偶数または奇数の整数値に設定し、鍵データを埋め込むものである。なお、MRA の変換係数を読み出す予め定めた順序は、埋め込みを行うためのキー情報であり、鍵データを抽出する際にも用いる。また、鍵データを暗号化および誤り訂正符号を付加したデジタル情報に変換し、そのデジタル情報を埋め込むようにしてもよい。さらに、埋め込むデジタル情報のビット数が、MRA の変換係数より少

ない場合は、例えば、デジタル情報を一通り埋め込んだ後に当該デジタル情報の第 1 ビットに戻って引き続き埋め込む。

【0034】

次に、認証データ埋込み部 1 4 の処理（ステップ S 3 0 4）について図 7 を参照して説明する。図 7 は、認証データ埋込み部 1 4 の一例を示すブロック図である。帯域分割部 1 1 で分割した信号の M R R の中から図 4 で示した L H 3 の変換係数 W_i を予め定めた順序で読み出し、比較器 5 1 に入力として与える。比較器 5 1 では、変換係数の絶対値 $|W_i|$ が予め定めた設定値 T 以上であるか否かを判定する。

【0035】

この判定において変換係数の絶対値が設定値 T 未満である場合には、第 1 の埋込み部 5 2 において、認証データ作成部 1 2 で作成した変換係数に対応する認証データのビット値に応じて、変換係数 W_i を小さな正の数 m または $-m$ に設定する（正の数 m は設定値 T より小さな値である）。

【0036】

これに対し、上記判定において変換係数の絶対値が設定値 T 以上である場合には、第 2 の埋込み部 5 3 において鍵情報埋込み部 1 3 と同様に、変換係数 W_i を量子化ステップサイズ Q で割った値を q とすると、変換係数に対応する認証データのビット値に応じて、 q の値を最も近い偶数または奇数の整数値に設定する。

【0037】

以上の処理を行い、変換係数 W_i に認証データのビット値を埋め込み、埋め込み処理された変換係数 W_i' を作成する。

【0038】

上記に続いて、L H 2 の変換係数を予め定めた順序で読み出し、比較器 5 1 に入力として与える。以降の処理は、L H 3 の変換係数に対するものと同様である。なお、ここでは、L H 3 の変換係数に対する処理に続いて、L H 2 の変換係数に対する処理を行ったが、この処理の順序は、L H 3 の変換係数に対する処理を先に行ってもよい。L H 3 と L H 2 の処理順序、および L H 3、L H 2 の変換係数を読み出すための予め定めた順序は、埋め込み処理を行うためのキー情報であ

り、情報を抽出する際にも用いる。また、L H 2 と L H 3 の変換係数を比較する設定値 T は、必ずしも同一でなくてもよい。好ましくは、L H 3 の変換係数を比較する設定値は、L H 2 の変換係数を比較する設定値より小さくする方がよい。例えば、L H 3 の変換係数を比較する設定値は 7、L H 2 の変換係数を比較する設定値は 1 0、m は 2 などと決めておく。

【 0 0 3 9 】

次に、帯域合成部 1 5 の処理について、図 8 および図 9 を用いて説明する。図 8 は、図 1 の帯域合成部 1 5 の構成の一例を示すブロック図である。帯域合成部 1 5 は、それぞれ同じ構成を有する第 1 ～第 3 の帯域合成フィルタ 4 0 0、5 0 0 および 6 0 0 を備える。第 1 ～第 3 の帯域合成フィルタ 4 0 0、5 0 0 および 6 0 0 は、4 つの周波数帯域信号を入力し、1 つの信号に合成して出力する（ステップ S 3 0 5）。

【 0 0 4 0 】

第 1 の帯域合成フィルタ 4 0 0 は、L L 3 信号、L H 3 信号、H L 3 信号および H H 3 信号とを入力し、これらを合成して L L 2 信号を作成する。第 2 の帯域合成フィルタ 5 0 0 は、上記合成した L L 2 信号と L H 2 信号、H L 2 信号および H H 2 信号とを入力し、これらを合成して L L 1 信号を作成する。そして、第 3 の帯域合成フィルタ 6 0 0 は、上記合成した L L 1 信号と L H 1 信号、H L 1 信号および H H 1 信号とを入力し、これらを合成してデジタル画像信号 7 2 を再構成する。

【 0 0 4 1 】

図 9 は、第 1 の帯域合成フィルタ 4 0 0 の構成の一例を示すブロック図である。図 9 において、第 1 の帯域合成フィルタ 4 0 0 は、第 1 ～第 3 の 2 帯域合成部 4 0 1 ～4 0 3 を備える。この第 1 ～第 3 の 2 帯域合成部 4 0 1 ～4 0 3 は、それぞれ L P F 4 1 1 ～4 1 3 と、H P F 4 2 1 ～4 2 3 と、信号に対して 2 : 1 の割合で零を挿入するアップサンプラ 4 3 1 ～4 3 3 および 4 4 1 ～4 4 3 と、加算器 4 5 1 ～4 5 3 とを備える。

【 0 0 4 2 】

第 1 の 2 帯域合成部 4 0 1 は、L L 3 信号と L H 3 信号とを入力して、それぞ

れアップサンプラ 4 3 1 および 4 4 1 を用いて 2 倍のサイズの信号に変換し、変換した 2 つの信号を垂直方向成分に関して L P F 4 1 1 および H P F 4 2 1 でフィルタリングした後、加算して出力する。

【 0 0 4 3 】

一方、第 2 の 2 帯域合成部 4 0 2 は、H L 3 信号と H H 3 信号とを入力して、それぞれアップサンプラ 4 3 2 および 4 4 2 を用いて 2 倍のサイズの信号に変換し、変換した 2 つの信号を垂直方向成分に関して L P F 4 1 2 および H P F 4 2 2 でフィルタリングした後、加算して出力する。

【 0 0 4 4 】

そして、第 3 の 2 帯域合成部 4 0 3 は、加算器 4 5 1 および 4 5 2 の出力を入力して、それぞれアップサンプラ 4 3 3 および 4 4 3 を用いて 2 倍のサイズの信号に変換し、変換した 2 つの信号を水平方向成分に関して L P F 4 1 3 および H P F 4 2 3 でフィルタリングした後、加算して出力する。

【 0 0 4 5 】

これにより、第 1 の帯域合成フィルタ 4 0 0 からは、第 2 の階層信号である水平・垂直方向共に低域の L L 2 信号が出力される。なお、第 2 および第 3 の帯域合成フィルタ 5 0 0 および 6 0 0 も、入力する信号に対して上記と同様の処理を行う。帯域合成部 1 5 は、上述のように L L 3 信号、L H 3 信号、H L 3 信号、H H 3 信号、L H 2 信号、H L 2 信号、H H 2 信号、L H 1 信号、H L 1 信号および H H 1 信号の 1 0 個の周波数帯域信号を、埋め込み処理が行われたデジタル画像信号 7 2 に再構成して出力する。

【 0 0 4 6 】

次に、情報抽出装置 2 a が行う情報抽出方法について図 2 と図 1 0 を参照して説明する。図 1 0 は、図 2 の情報抽出装置 2 a で行う処理を示すフローチャートである。帯域分割部 1 1 は、デジタル画像信号 7 3 を入力する。このデジタル画像信号 7 3 は、上記情報埋込み装置 1 a の帯域合成部 1 5 が出力するデジタル画像信号 7 2 が送信途中で、圧縮符号化・伸長化の処理、あるいは改ざん処理が施された信号である。帯域分割部 1 1 は、入力されたデジタル画像信号 7 3 に関して離散ウェーブレット変換を行って 1 0 個の周波数帯域 L L 3 信号、L H 3 信号

、HL 3 信号、HH 3 信号、LH 2 信号、HL 2 信号、HH 2 信号、LH 1 信号、HL 1 信号およびHH 1 信号に分割し、それぞれの変換係数を算出する（ステップS 1 0 0 1）。

【0 0 4 7】

次に、鍵情報抽出部 2 1 は、帯域分割部 1 1 で分割したMRA成分の変換係数から情報埋込み装置 1 a の鍵情報埋込み部 1 3 で行ったのと同じ順序で読み出し、埋め込まれている鍵情報を抽出する（ステップS 1 0 0 2）。この抽出手法は、特開平 1 1 - 1 9 6 2 6 2 号公報に開示された技術を用いる。すなわち、変換係数を量子化ステップサイズQで割った値を四捨五入した値をpとすると、前記pの値が偶数か奇数かを判定し、当該判定の結果に基づいて埋込まれた情報のビット値を抽出する。

【0 0 4 8】

次に、鍵情報判定部 2 2 は、鍵情報抽出部 2 1 で抽出した情報が、情報埋込み装置 1 a において用いた鍵データと同一であるか否かの正当性を判定する（ステップS 1 0 0 3）。例えば、鍵データに含まれる初期値、乱数発生関数の種類、系列のビット長の各値をそれぞれ情報埋込み装置と情報抽出装置の双方で予め複数個の候補を決めておく。

【0 0 4 9】

もし抽出した情報がその候補値といずれも一致しない場合、同一でないと判定するようにする。このステップS 1 0 0 3における判定の結果、正しいと判断した場合は、ステップS 1 0 0 4以降の処理を行う。一方、ステップS 1 0 0 3における判定の結果、正しくないと判断した場合は、デジタル画像信号 7 3 には改ざん有りと検出する（ステップS 1 0 1 1）。

【0 0 5 0】

この判定部は必須ではないが、鍵データの正当性を判定することにより、本発明の改ざん防止装置における信頼性が増して、実用上好ましい。次に、認証データ作成部 1 2 は、前記鍵データを用いて疑似乱数系列を作成し、当該疑似乱数系列から認証データKを作成する（ステップS 1 0 0 4）。

【0 0 5 1】

次に、埋込み情報抽出部 2 3 の処理（ステップ S 1 0 0 5）について図 2 と図 1 1 を参照して説明する。図 1 1 は、埋込み情報抽出部 2 3 の一例を示すブロック図である。帯域分割部 1 1 で分割した M R R 成分の中から L H 3、L H 2 の変換係数を情報埋込み装置 1 a の認証データ埋込み部 1 4 で行ったのと同じ順序、すなわち、L H 3、L H 2 の順に認証データ埋込み部 1 4 と同一の予め定めた順序で読み出す。読み出された変換係数 W_i は、比較器 5 1 に入力され、変換係数の絶対値 $|W_i|$ が予め定めた設定値 T 以上であるか否かを判定する。

【0 0 5 2】

この判定において変換係数の絶対値が設定値 T 未満である場合には、第 1 の抽出部 5 4 において、変換係数の値が正か負かを判定し、当該判定の結果に基づいて変換係数毎に埋込まれた埋込み情報のビット値を抽出する。

【0 0 5 3】

これに対し、変換係数の絶対値が設定値 T 以上である場合には、第 2 の抽出部 5 5 において、上記鍵情報抽出部 2 1 と同様に、変換係数を量子化ステップサイズ Q で割り四捨五入した値を p とすると、前記 p の値が偶数か奇数かを判定し、当該判定の結果に基づいて変換係数毎に埋込まれた埋込み情報のビット値を抽出する。以上の処理を行い、埋込み情報 D を抽出する（ステップ S 1 0 0 5）。

【0 0 5 4】

次に、領域対応埋込情報読出部 2 4 と領域対応認証データ読出部 2 5 の処理について、図 2 と図 1 2 を参照して説明する。図 1 2 は、デジタル画像信号 7 3 を 32×32 画素サイズのブロックに分割した場合、画像中の左上のブロックと同一の空間的領域を表現する L H 3 と L H 2 の変換係数を示している（図 1 2 中の太い実線の枠線部分に対応する）。

【0 0 5 5】

すなわち、L H 3 と L H 2 の各ブロックサイズは、それぞれ縦横 4×4 画素、 8×8 画素である。今、L H 3、L H 2 の変換係数を読み出す予め定めた順序が、縦横 1 つ毎に読み出した場合、L H 3 内の 4 個と L H 2 内の 16 個が各ブロックの位置と同一の空間的領域を表現する変換係数内に埋め込まれている埋込み情報の系列である（図 1 2 中、黒で塗りつぶした部分である）。

【0056】

従って、領域対応埋込情報読出部 24 では、埋込み情報抽出部 23 で抽出した埋込み情報 D の中から、上記 20 個の埋込み情報の系列 BD を読み出す（ステップ S1006）。

【0057】

同様に、領域対応認証データ読出部 25 では、認証データ作成部 12 で作成した認証データ K の中から、埋込み情報の系列 BD と同じ位置に対応する 20 個の認証データの系列 BK を読み出す（ステップ S1007）。

【0058】

例えば、図 12 において、LH3 と LH2 の左上のブロックに埋め込まれている埋込み情報の系列 BD が、 $BD = \{1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1\}$ で、認証データの系列 BK が、 $BK = \{1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1\}$ であるとする。この例では、2、4、12、14 番目のビットが 4 箇所異なっている。

【0059】

次に、ブロック改ざん判定部 26 は、上記読み出したビット列 BD と BK との排他的論理和の総和を求める（ステップ S1008）。

【0060】

その求めた値 S と予め定めた設定値 BT を比較することにより、ブロックに分割した部分画像（ここでは、 32×32 画素サイズのブロック）に対して改ざんが行われている否かを判定する（ステップ S1009）。

【0061】

例えば、求めた値 S が予め定めた設定値 BT より大きい場合は、改ざんが行われていると判定し、反対に小さい場合は、改ざんが行われていないと判定する。排他的論理和の例を説明したのが図 13 である。お互いのビットの値が相異なる場合は値 1 を出力し、同じビット値同士の場合は値 0 を出力する。上記のビット列 BD と BK に適用した場合、出力値 S は 4 となる。予め定めた設定値 BT が 3 である場合は、値 S が設定値 T より大きいため、当該ブロックは改ざんが行われ

ていると判定される。

【0062】

なお、排他的論理和の総和を求める代わりに、ビット列BDとBKの20個のビット値の一致している個数または内積を求めて比較してもよい。また、ビット値を0のかわりに-1として内積を計算してもよい。このステップS1009における判定の結果、改ざんがあると判断した場合は、前記ブロックに対応する位置を改ざん有りメモリに格納（図示せず）またはディスプレイに表示（図示せず）する（ステップS1011）。

【0063】

一方、ステップS1009における判定の結果、改ざんが無いと判断した場合は、前記ブロックに対応する位置を改ざん無しメモリに格納（図示せず）またはディスプレイに表示（図示せず）する（ステップS1010）。

【0064】

以上のステップS1006からステップS1009の処理を、全てのブロックに対して繰り返し行うことにより、デジタル画像中の改ざん部分の位置を検出する。

【0065】

以上のように、本実施形態に係る改ざん防止装置によれば、3階層に帯域分割を行い、MRRの中からLH3、LH2の全体の変換係数に認証データを埋め込む。しかも、認証データは、鍵データを用いて疑似乱数系列から作成し、その鍵データはMRAの変換係数に埋め込む。さらに、画像を予め定めた複数の画素から構成される複数のブロックに分割し、各ブロックと同一の空間的領域を表現するMRRの変換係数内に埋め込んだ埋込み情報を読み出し、実際に埋め込んだ認証データと比較照合することにより、デジタル画像中の改ざん部分の位置を検出することができる。

【0066】

従って、比較的低周波成分の変換係数に情報を埋め込むことにより、非可逆的な圧縮符号化を行っても埋め込んだ鍵データと認証データは保持される。すなわち、非可逆的な圧縮と画像の一部を改ざんする行為とを区別することができ、しか

も改ざん部分の特定が可能なデジタル画像の改ざん防止装置を実現できる。

【0067】

なお、本実施形態に係る改ざん防止装置において行う離散ウェーブレット変換は、3つの階層に限られるものではなく、LL信号が1×1の要素になるまで何回でも階層化してよい。また、認証データを埋め込みに用いる帯域はLH3、LH2に限ったものではなく、MR Rの中から任意の帯域を選択して用いてもよく、またMR R全域を用いてもよい。この場合、帯域の変換係数に対する処理の順序は、いずれの順序でもよいが、その順序は予め定めておく必要がある。

【0068】

ただし、本発明においては、より深い階層信号のみの変換係数に認証データを埋め込むのが最も好ましく、例えば、図4において、第3の階層信号のLH3信号とHL3信号、第2の階層信号のLH2信号とHL2信号の全てもしくはその一部から構成した数列に埋め込むようにしている。

【0069】

また、認証データは、認証データ埋込み部14において予め定めた順序で読み出された変換係数毎に順番に埋め込むようにしているが、複数のブロックに分割した各ブロックと同一の空間的領域を表現するMR R内に埋め込む認証データは、ブロック毎に同じ認証データを繰り返し埋め込むようにしてもよい。

【0070】

なお、情報埋込み装置において鍵データを公開鍵暗号または共通鍵暗号を行って暗号化して埋め込み、情報抽出装置において暗号化された情報を復号する場合は、両装置間で予め公開鍵または共通鍵を決定しておく必要がある。

【0071】

なお、典型的には、上記の実施形態に係る改ざん防止装置が実現する各機能は、所定のプログラムデータが格納された記憶装置（ROM，RAM，ハードディスク等）と、当該プログラムデータを実行するCPU（セントラル・プロセッシング・ユニット）とによって実現される。この場合、各プログラムデータは、CD-ROMやフロッピーディスク等の記録媒体を介して導入されてもよい。

【0072】

【発明の効果】

本発明によれば、デジタル画像中のどの位置が改ざんされたのかを領域別に特定することができる。また、非可逆的な圧縮符号化を行っても埋め込んだ鍵データと認証データが保持されるので、非可逆的な画像圧縮と画像の一部を改ざんするような行為とを区別することができる。しかも、埋め込まれた周波数帯域の情報、具体的に用いた変換係数、変換係数の読み出し順序、および鍵データの情報を知らない第三者による認証データの解読が困難なため、埋め込み情報の上書きやすき替えは不可能である。

【図面の簡単な説明】

【図 1】

本発明の実施形態に係る改ざん防止装置の情報埋込み装置の構成図

【図 2】

本発明の実施形態に係る改ざん防止装置の情報抽出装置の構成図

【図 3】

図 1 の情報埋込み装置で行う処理のフローチャート

【図 4】

図 1 の帯域分割部の構成を示すブロック図

【図 5】

図 4 の第 1 の帯域分割フィルタの構成を示すブロック図

【図 6】

離散ウェーブレット変換による各信号の 2 次元周波数領域での表現図

【図 7】

図 1 の認証データ埋込み部の構成を示すブロック図

【図 8】

図 1 の帯域合成部の構成を示すブロック図

【図 9】

図 8 の第 1 の帯域合成フィルタの構成を示すブロック図

【図 10】

図 2 の情報抽出装置で行う処理のフローチャート

【図 1 1】

図 2 の埋込み情報抽出部の構成を示すブロック図

【図 1 2】

3 2 × 3 2 画素サイズのブロックと同一の空間的領域を表現する L H 3 と L H
2 の変換係数の模式図

【図 1 3】

排他的論理和の例の説明図

【図 1 4】

従来の電子認証手順の説明図

【符号の説明】

- 1 a 情報埋込み装置
- 2 a 情報抽出装置
- 1 1 帯域分割部
- 1 2 認証データ作成部
- 1 3 鍵情報埋込み部
- 1 4 認証データ埋込み部
- 1 5 帯域合成部
- 2 1 鍵情報抽出部
- 2 2 鍵情報判定部
- 2 3 埋込み情報抽出部
- 2 4 領域対応埋込情報読出部
- 2 5 領域対応認証データ読出部
- 2 6 ブロック改ざん判定部
- 5 1 比較器
- 5 2 第 1 の埋込み部
- 5 3 第 2 の埋込み部
- 5 4 第 1 の抽出部
- 5 5 第 2 の抽出部
- 7 1, 7 2, 7 3 デジタル画像信号

1 0 0, 2 0 0, 3 0 0 帯域分割フィルタ

1 0 1 ~ 1 0 3 2 帯域分割部

1 1 1 ~ 1 1 3, 4 1 1 ~ 4 1 3 1 次元の低域通過フィルタ (L P F)

1 2 1 ~ 1 2 3, 4 2 1 ~ 4 2 3 1 次元の高域通過フィルタ (H P F)

1 3 1 ~ 1 3 3, 1 4 1 ~ 1 4 3 ダウンサンプラ

4 0 0, 5 0 0, 6 0 0 帯域合成フィルタ

4 0 1 ~ 4 0 3 2 帯域合成部

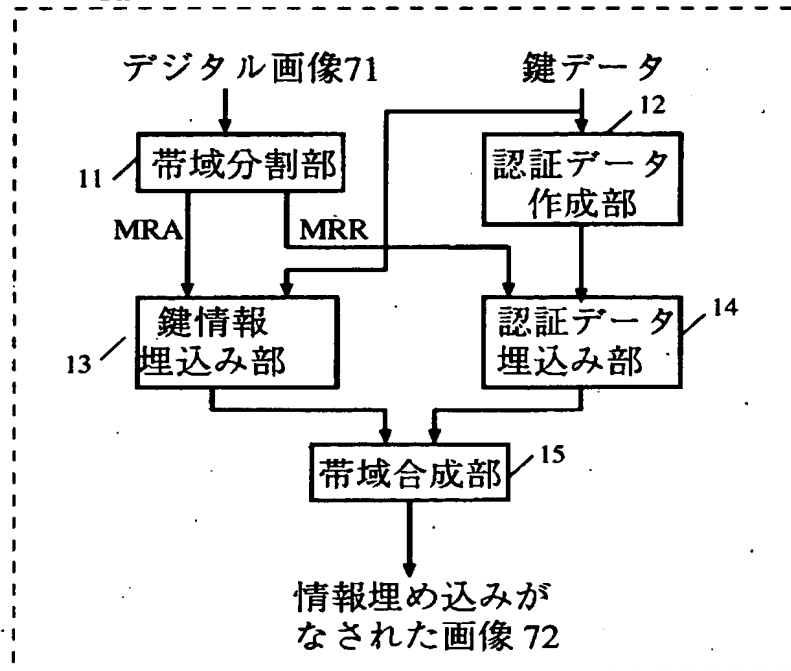
4 3 1 ~ 4 3 3, 4 4 1 ~ 4 4 3 アップサンプラ

4 5 1 ~ 4 5 3 加算器

【書類名】 図面

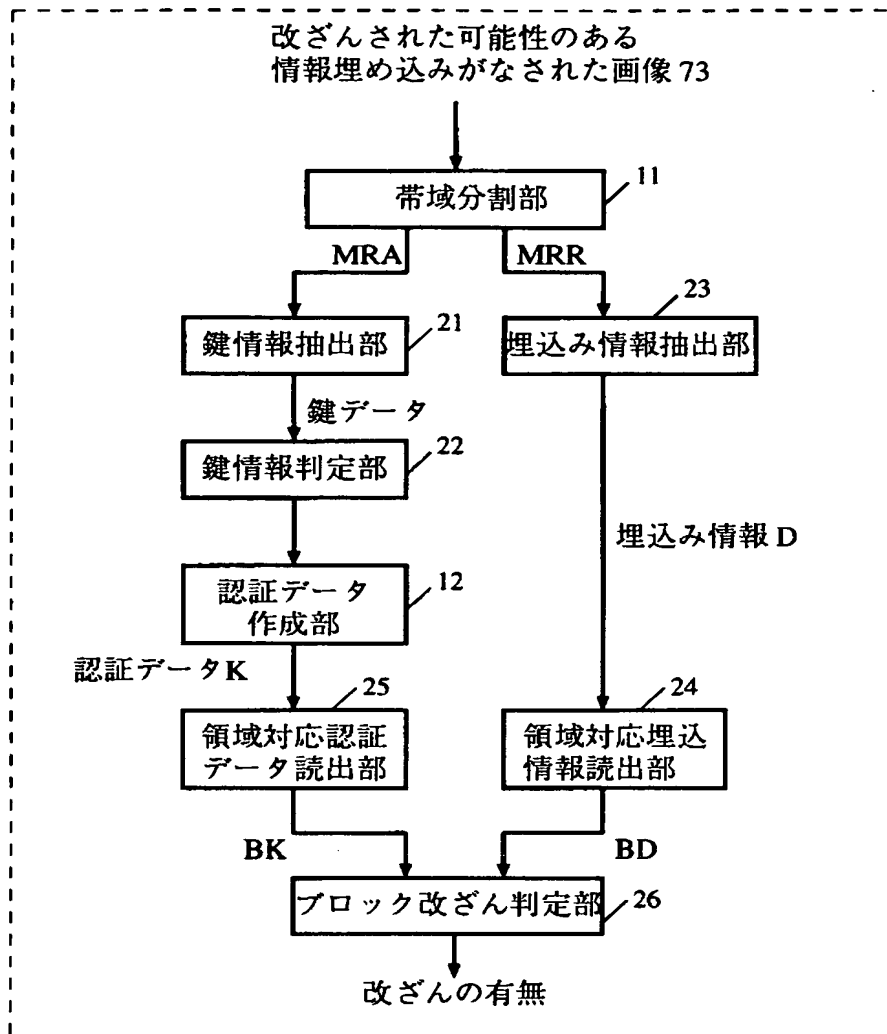
【図 1】

情報埋込み装置 1a

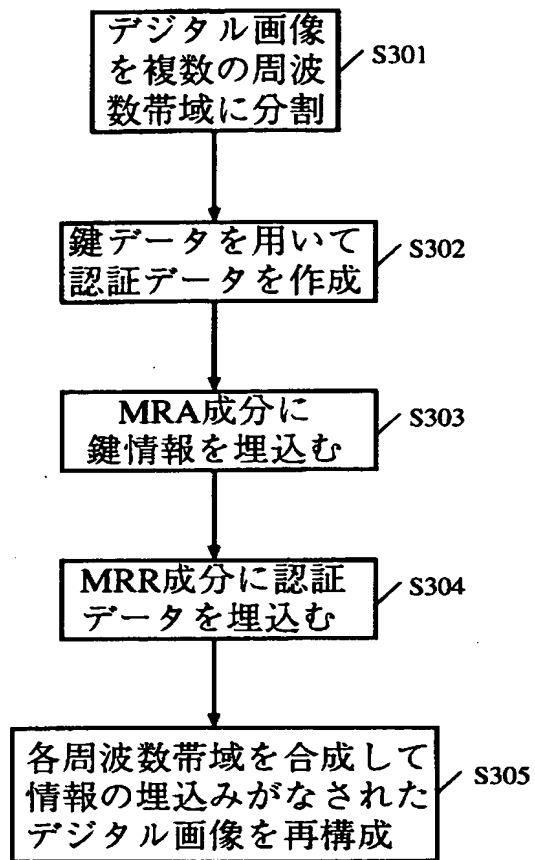


【図 2】

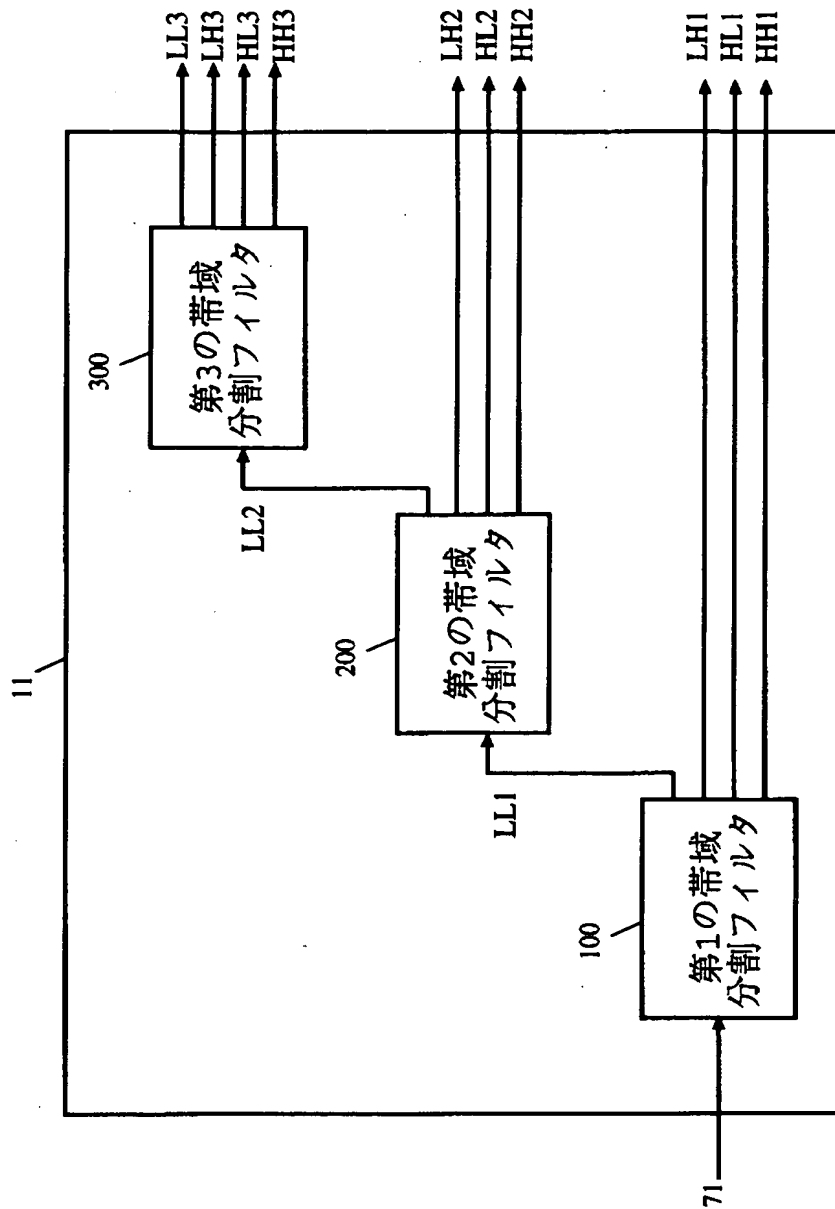
情報抽出装置2a



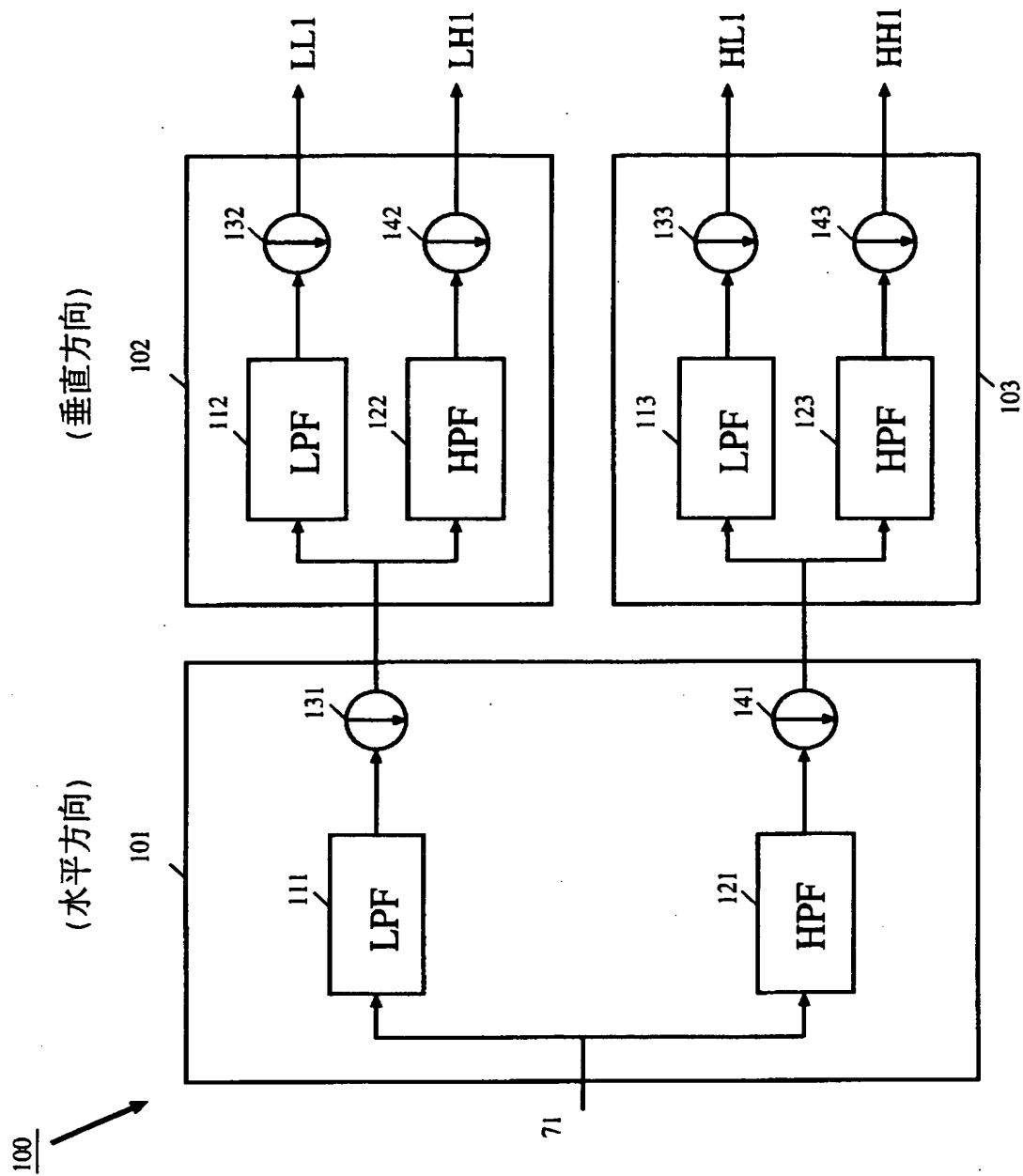
【図 3】



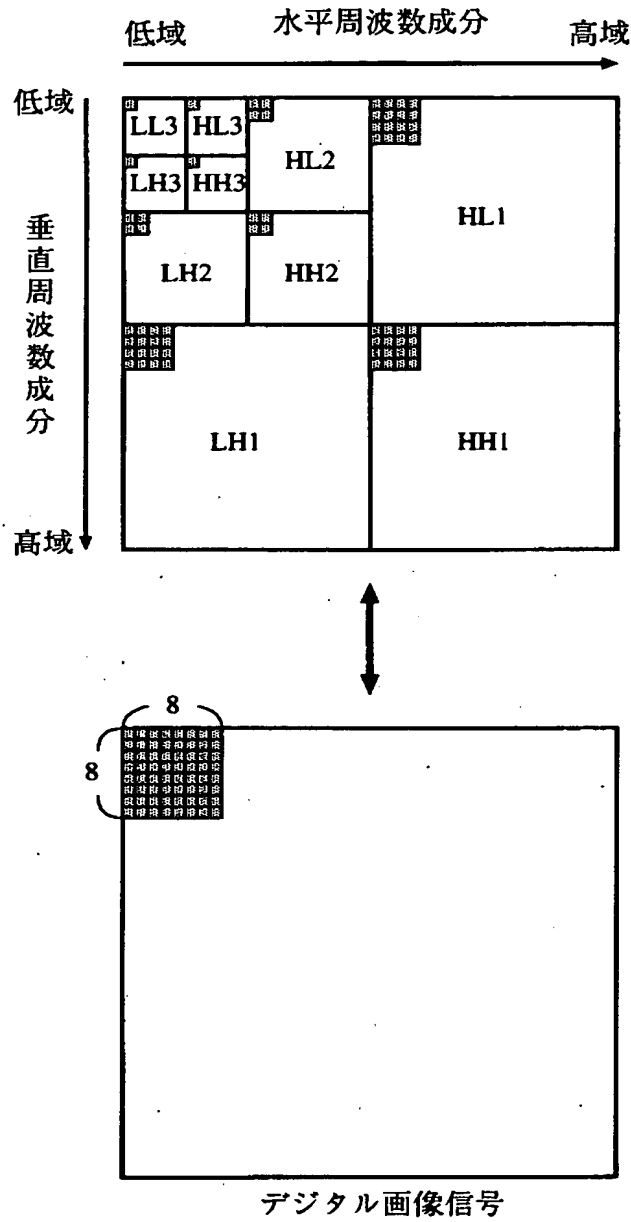
【図 4】



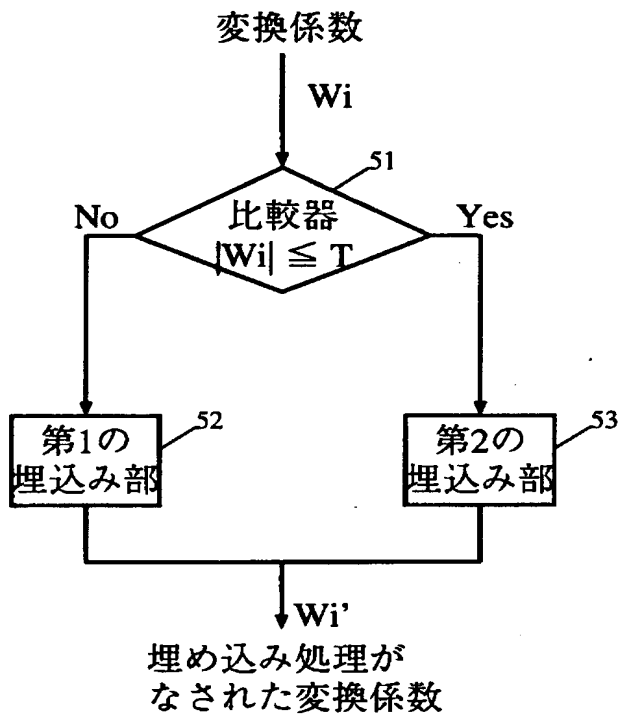
【図 5】



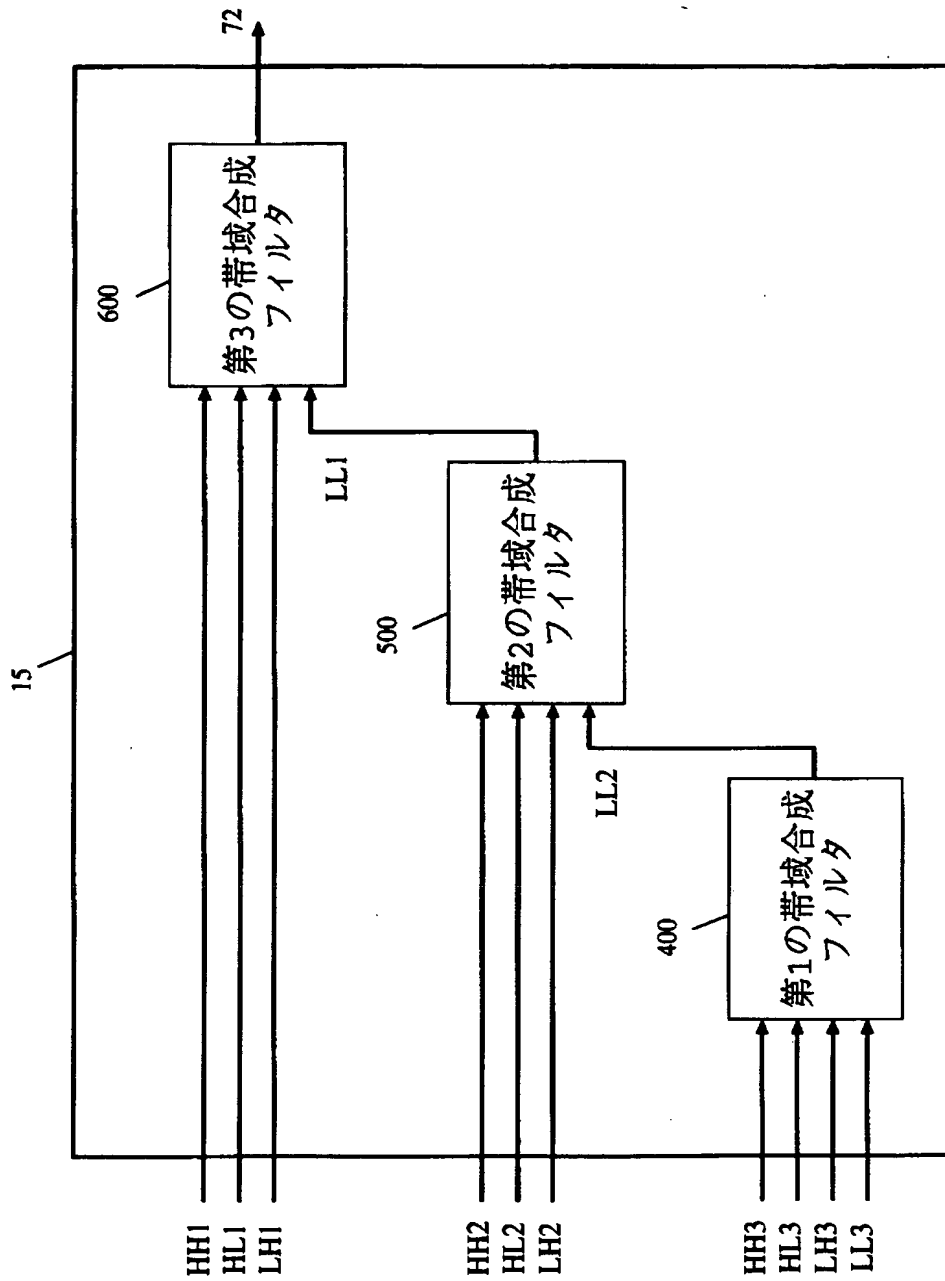
【図 6】



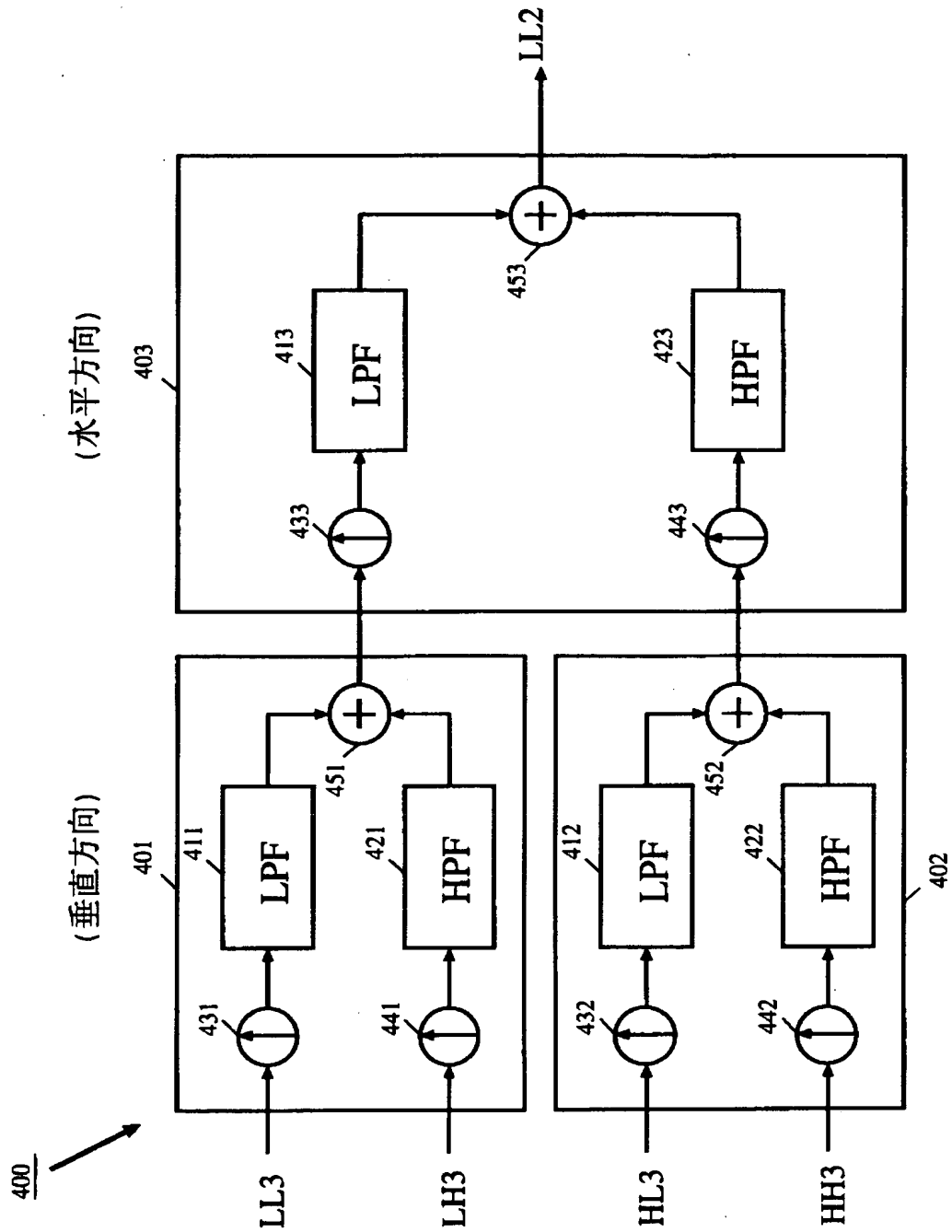
【図 7】



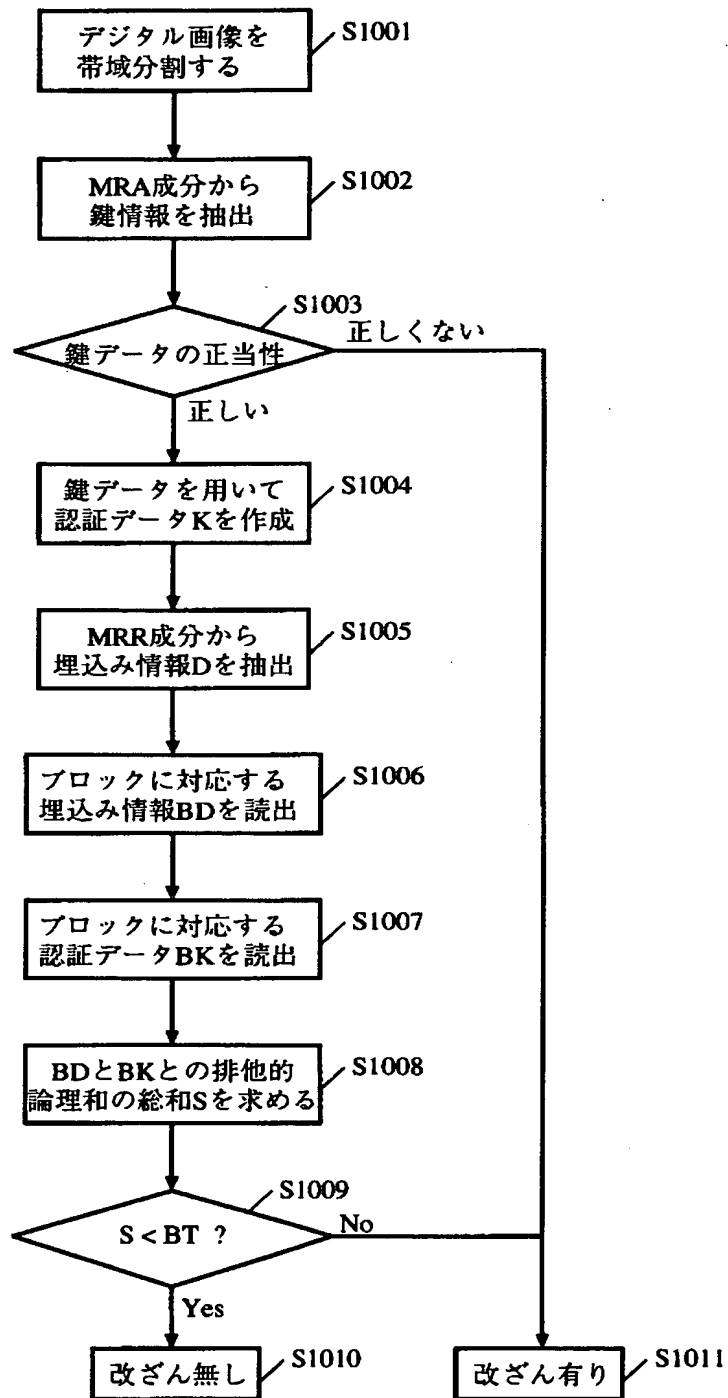
【図 8】



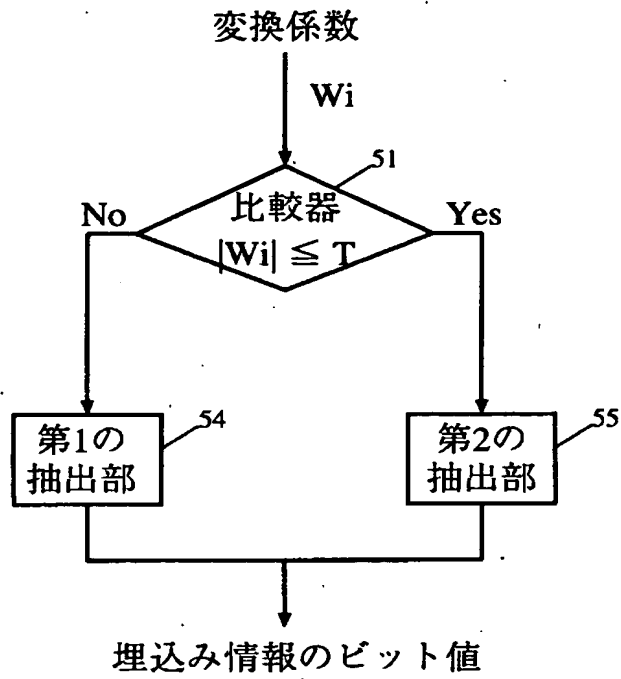
【图 9】



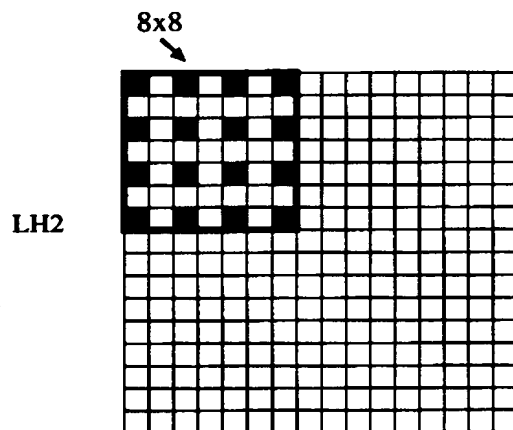
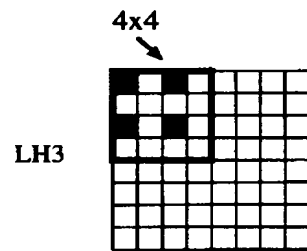
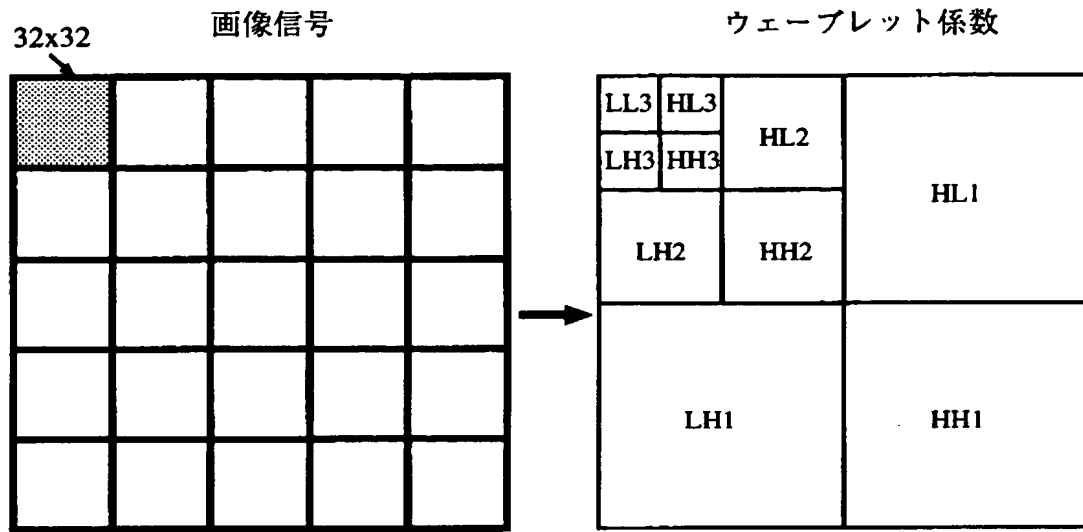
【図 1 0】



【図 1 1】



【図 1 2】



【図 1 3】

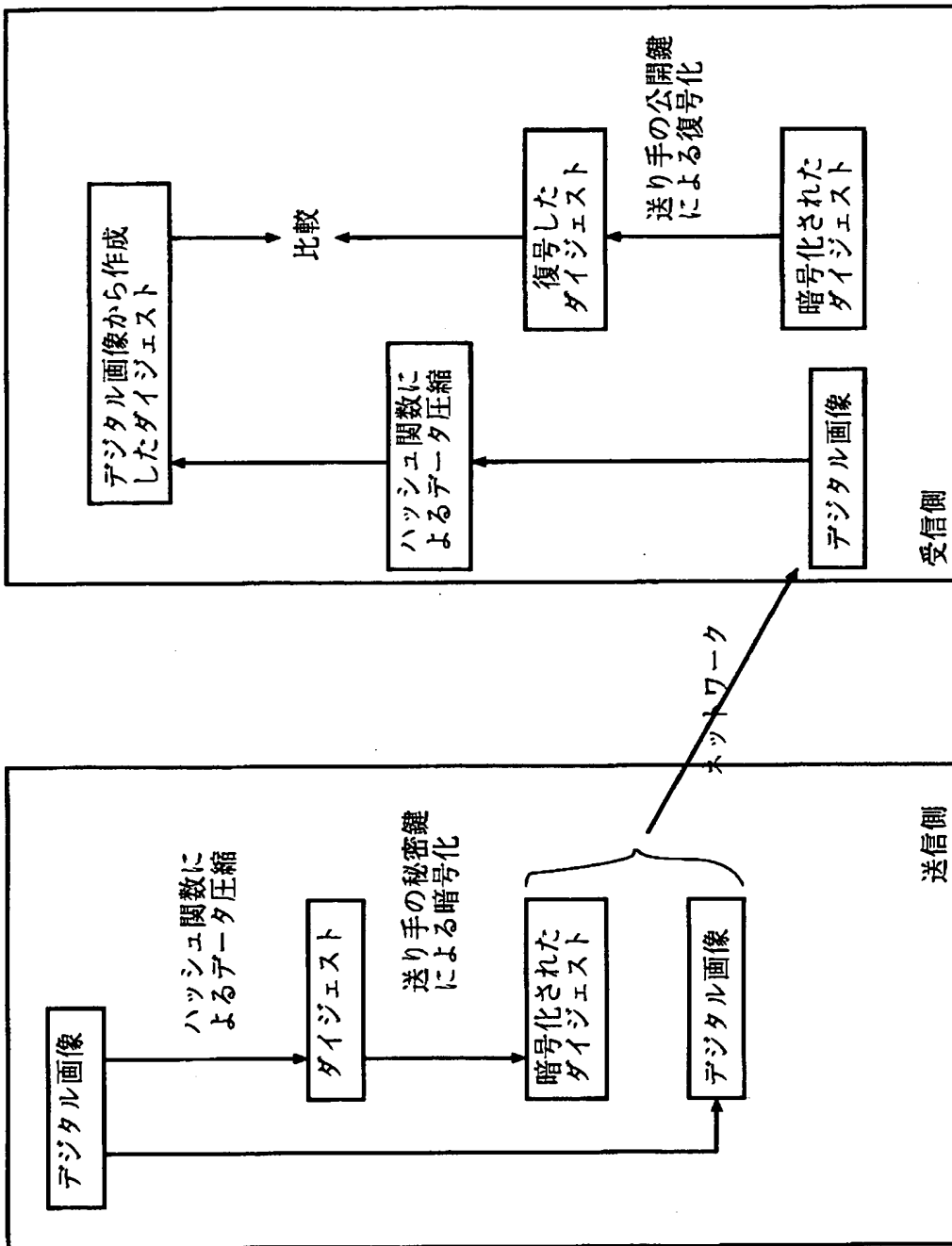
$$0 \times 0 = 0$$

$$0 \times 1 = 1$$

$$1 \times 0 = 1$$

$$1 \times 1 = 0$$

【図 1 4】



【書類名】 要約書

【要約】

【課題】 画像圧縮と改ざん行為とを区別でき、画像中のどの位置が改ざんされたのかを領域別に特定することができる。

【解決手段】 情報埋込み装置では、画像を複数の周波数帯域に分割し変換係数を算出する。鍵データを用いて疑似乱数系列を作成し認証データを作成する。鍵データはMRA、認証データはMRRの変換係数に埋込む。埋込み処理されたMRAとMRRを合成し情報が埋込まれた画像を再構成する。情報抽出装置では、画像を帯域分割したMRAから鍵データを抽出し、本来埋込んである認証データを作成する。MRRから埋込み情報を抽出する。画像を予め定めた複数の画素から構成される複数のブロックに分割し、各ブロックと同一の空間的領域を表現するMRRの変換係数内に埋込まれている埋込み情報の系列とそれに対応する認証データの系列とを比較照合することにより、領域毎の改ざんの有無を判定する。

【選択図】 図 2

出 願 人 履 歴 情 報

識別番号 [000005821]

1. 変更年月日 1990年 8月28日
[変更理由] 新規登録
住 所 大阪府門真市大字門真1006番地
氏 名 松下電器産業株式会社